(12) DEMANDE INTERNATIONALE PUBLIÉE EN VERTU DU TRAITÉ DE COOPÉRATION EN MATIÈRE DE BREVETS (PCT)

(19) Organisation Mondiale de la Propriété Intellectuelle
Bureau international

(43) Date de la publication internationale
28 août 2003 (28.08.2003)

PCT

(10) Numéro de publication internationale
WO 03/071733 A1

(51) Classification internationale des brevets[7] : H04L 9/06

(21) Numéro de la demande internationale :
PCT/FR03/00369

(22) Date de dépôt international : 6 février 2003 (06.02.2003)

(25) Langue de dépôt : français

(26) Langue de publication : français

(30) Données relatives à la priorité :
02/01883 15 février 2002 (15.02.2002) FR

(71) Déposant *(pour tous les États désignés sauf US)* : **GEMPLUS** [FR/FR]; Avenue du Pic de Bertagne, Parc d'activités de Gémenos, F-13420 GEMENOS (FR).

(72) Inventeurs; et

(75) Inventeurs/Déposants *(pour US seulement)* : **BRIER, Eric** [FR/FR]; Villa La Bergène, 5 Avenue des Pinsons, F-13600 LA CIOTAT (FR). **CLAVIER, Christophe** [FR/FR]; 1657 chemin des Solans, F-13400 AUBAGNE (FR).

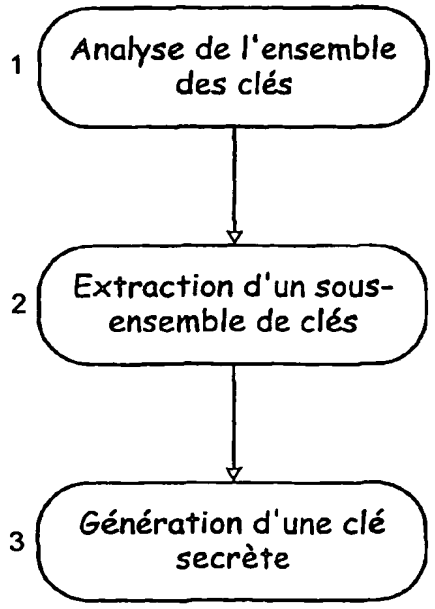
(74) Mandataire : **BRUYERE, Pierre**; C/O GEMPLUS, LA VIGIE, Service Brevets, BP 90, F-13705 LA CIOTAT CEDEX (FR).

(81) États désignés *(national)* : AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, OM, PH, PL, PT, RO, RU, SC, SD, SE, SG,

[Suite sur la page suivante]

(54) Title: METHOD FOR GENERATING SECURE KEYS FOR A CRYPTOGRAPHIC ALGORITHM

(54) Titre : PROCEDE DE GENERATION DE CLES SECURISEES POUR UN ALGORITHME CRYPTOGRAPHIQUE



1...THE WHOLE SET OF KEYS IS ANALYZED
2...A SUBSET OF KEYS IS EXTRACTED
3...AN ENCODED KEY IS GENERATED

(57) **Abstract:** The invention relates to a method and a corresponding device for generating secret secure keys for a cryptographic algorithm. The inventive method comprises the following steps: E1) the whole set (IK) of possible keys is analyzed; E2) a subset (SK) of keys is extracted; E3) the secret keys are generated on the basis of the subset of keys.

(57) **Abrégé :** L'invention concerne un procédé et dispositif associé de génération de clés secrètes sécurisées pour un algorithme cryptographique.Selon l'invention, le procédé comprend les étapes suivantes :E1 : analyse de l'ensemble (IK) des clés possibles ;E2 : extraction d'un sous ensemble (SK) de clés ;E3 : génération des clés secrètes ô partir du sous-ensemble de clés.

WO 03/071733 A1

SK, SL, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) **États désignés** *(régional)* : brevet ARIPO (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), brevet eurasien (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), brevet européen (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PT, SE, SI, SK, TR), brevet OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Déclarations en vertu de la règle 4.17 :

— *relative à l'identité de l'inventeur (règle 4.17.i)) pour les désignations suivantes AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, OM, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, TJ, TM, TN, TR, TT, TZ, UA, UG, UZ, VC, VN, YU, ZA, ZM, ZW, brevet ARIPO (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), brevet eurasien (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), brevet européen (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PT, SE, SI, SK, TR), brevet OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG)*

— *relative au droit du déposant de demander et d'obtenir un brevet (règle 4.17.ii)) pour les désignations suivantes AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, OM, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, TJ, TM, TN, TR, TT, TZ, UA, UG, UZ, VC, VN, YU, ZA, ZM, ZW, brevet ARIPO (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), brevet eurasien (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), brevet européen (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PT, SE, SI, SK, TR), brevet OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG)*

— *relative au droit du déposant de revendiquer la priorité de la demande antérieure (règle 4.17.iii)) pour toutes les désignations*

— *relative à la qualité d'inventeur (règle 4.17.iv)) pour US seulement*

Publiée :

— *avec rapport de recherche internationale*

— *avant l'expiration du délai prévu pour la modification des revendications, sera republiée si des modifications sont reçues*

En ce qui concerne les codes à deux lettres et autres abréviations, se référer aux "Notes explicatives relatives aux codes et abréviations" figurant au début de chaque numéro ordinaire de la Gazette du PCT.

PROCEDE DE GENERATION DE CLES SECURISEES POUR UN ALGORITHME CRYPTOGRAPHIQUE

L'invention concerne un procédé de génération de clés sécurisées pour un algorithme cryptographique. L'invention, très générale, peut être utilisée pour sécuriser tout algorithme cryptographique totalement ou partiellement cassé.

Les algorithmes cryptographiques sont le plus souvent utilisés dans des applications où l'accès à des données ou à des services est sévèrement contrôlé. Ces algorithmes sont notamment utilisés dans les cartes à puce pour certaines applications de celles-ci. Ce sont par exemple des applications d'accès à certaines banques de données, des applications bancaires, des applications de télépéage, par exemple pour la télévision, la distribution d'essence ou encore le passage de péages d'autoroute. Ces algorithmes sont également utilisés dans les cartes dites cartes SIM, pour des applications de téléphonie mobile.

Les algorithmes cryptographiques sont généralement mis en oeuvre dans des composants électroniques ayant une architecture formée autour d'un microprocesseur et de mémoires, dont une mémoire non volatile qui contient la clé secrète.

De manière générale et succinte, ces algorithmes ont pour fonction de calculer un message chiffré à partir de la clé secrète contenue dans la carte et d'un message en clair appliqué en entrée (du composant) par un système hôte (serveur à distance, distributeur bancaire, etc.), et de fournir en retour au système hôte le message chiffré obtenu. Ceci permet au système hôte d'authentifier le composant avant d'échanger des données. Le message chiffré est accessible depuis l'extérieur. Cependant, le message clair ne peut être retrouvé sans la connaissance de la clé secrète utilisée pour obtenir le message chiffré.

Les algorithmes cryptographiques les plus connus sont les algorithmes DES, AES et RSA. Dans le cadre de la

téléphonie mobile l'algorithme le plus utilisé est le Comp128. Cette liste n'est bien sûr pas exhaustive. Les caractéristiques des algorithmes cryptographiques sont supposées connues : opérations effectuées, paramètres utilisés. Seule reste inconnue la clé secrète qui est spécifique à chaque composant et qui ne peut être déduite de la seule connaissance du message clair et/ou du message chiffré.

L'invention peut s'appliquer aussi bien à un algorithme symétrique (tel que DES ou AES) qu'à un algorithme asymétrique (tel que RSA). On désigne par le terme "clé secrète" aussi bien la clé unique d'un algorithme symétrique que la clé privée d'un algorithme asymétrique.

Dans le cadre des algorithmes symétriques, la clé secrète est un nombre binaire dont la taille N0 dépend de l'algorithme utilisé. Par exemple, l'algorithme DES utilise des clés de N0=56 bits, l'algorithme Comp128 utilise des clés de N0=128 bits. Pour un tel algorithme, il existe donc un ensemble comprenant $N=2^{N0}$ clés possibles.

Au cours d'une phase de personnalisation du composant, une clé secrète est générée, qui est ensuite mémorisée dans une mémoire non volatile du composant. La génération de clé se fait de manière connue à partir d'un générateur de nombres aléatoires apte à produire des nombres de la taille N0 souhaitée.

Un composant et l'algorithme qu'il utilise peuvent être vulnérables à des analyses ayant pour but de "casser" l'algorithme, c'est à dire de trouver la clé secrète qu'il utilise. Une telle action, si elle aboutit, peut avoir des conséquences graves allant jusqu'au clonage du composant.

Ces analyses, du moins celles qui sont connues actuellement, sont essentiellement de deux types : la cryptanalyse et les attaques à canaux cachés (en anglais : side-channel attacks).

Une cryptanalyse consiste à mener un processus mathématique ou statistique n'utilisant que la connaissance de l'algorithme et d'une ou plusieurs paires clair/chiffré pour retrouver la clé secrète utilisée par cet algorithme.

Une attaque à canal caché consiste en une analyse simple ou différentielle (statistique) d'un paramètre physique spécifique lié au composant lorsqu'il exécute l'algorithme. Cette attaque repose sur le fait que la trace (la variation du paramètre physique spécifique, par exemple la consommation de courant, le rayonnement électromagnétique, etc.) du composant exécutant des instructions varie en fonction des données qu'il manipule, et donc en fonction de la clé secrète utilisée. En particulier, lorsque le composant exécute l'algorithme, la trace du composant dépend du message clair, de la clé secrète et/ou du message chiffré. A partir de mesures de cette trace et d'études statistiques de ces mesures, il est possible de retrouver la clé secrète.

Enfin, dans tous les cas de figure, une attaque par recherche exhaustive est possible. Elle consiste à rechercher la clé secrète de manière systématique. Pour cela, à partir d'un message clair et d'un message chiffré associé connu, l'algorithme est exécuté de manière systématique avec l'ensemble des clés, une à une, jusqu'à obtention de la clé secrète utilisée. La recherche exhaustive demande un temps très important (temps croissant de manière exponentielle avec la longueur en bits des clés) et/ou un matériel particulièrement performant pour être menée à terme.

Contrairement à la recherche exhaustive, la durée d'une cryptanalyse ou d'une attaque à canal caché peut dépendre de la valeur de la clé secrète.

La sécurité ou résistance d'un algorithme est sa capacité à résister à une attaque quelle qu'elle soit et quelle que soit la clé qu'il utilise. Un algorithme est dit sûr si le temps nécessaire pour le casser est prohibitif (de l'ordre de quelques semaines à quelques années).

La sécurité d'un algorithme augmente fortement avec la taille des clés utilisées. En revanche, la sécurité d'un algorithme diminue dans le temps car les performances des matériels susceptibles d'être utilisés pour le casser augmentent, de même que les connaissances d'éventuels attaquants.

Des solutions sont connues pour renforcer la sécurité d'un algorithme contre les attaques à canaux cachés : elles consistent à intervenir au niveau de l'implantation de l'algorithme et à le modifier de sorte que sa trace devienne imprédictible : par exemple, il est possible d'intervertir des étapes du procédé de manière aléatoire, de mélanger des données manipulées par l'algorithme avec un ou des paramètres aléatoires, etc.

Ces solutions sont efficaces. Cependant, elles sont plus ou moins difficiles à mettre en oeuvre car elles nécessitent de modifier en partie l'implantation de l'algorithme. Ces solutions sont également coûteuses en termes de temps d'exécution de l'algorithme, car le plus souvent le nombre total d'étapes de l'algorithme est augmenté.

S'il s'avère impossible ou non souhaitable de sécuriser par ces méthodes l'implantation d'un algorithme, il peut être envisagé de remplacer cet algorithme par un algorithme plus sûr. Cependant, ce remplacement dans un composant existant nécessite de surcroît de modifier l'infrastructure dans laquelle le composant s'inscrit, ce qui peut nécessiter des investissements techniques prohibitifs.

Au vu des problèmes exposés ci-dessus, un but de l'invention est de mettre en oeuvre un procédé de sécurisation d'un algorithme cryptographique particulièrement simple et peu onéreux.

Ainsi l'invention concerne un procédé de génération de clés secrètes sécurisées pour un algorithme cryptographique, le procédé étant caractérisé en ce qu'il comprend les étapes suivantes :

E1 : analyse de l'ensemble (IK) des clés possibles ;

E2 : extraction d'un sous-ensemble (SK) de clés à partir de l'ensemble (IK) ;

E3 : génération des clés secrètes à partir du sous-ensemble (SK) de clés.

L'invention est applicable pour tout algorithme cryptographique sensible à au moins une attaque identifiée, lorsque ledit algorithme se comporte différemment vis-à-vis de l'attaque identifiée selon la valeur de la clé qu'il utilise. Cela suppose que les notions de clé forte et de clé faible soient pertinentes pour l'attaques identifiée. Une clé est dite forte si le temps nécessaire, pour ladite clé, à l'aboutissement de l'attaque identifiée est prohibitif. Une clé est dite faible dans le cas contraire.

Selon l'invention, on génère ainsi des clés secrètes parmi un sous-ensemble de clés présélectionnées pour leur résistance à l'attaque identifiée. On diminue ainsi fortement les chances de réussite de cette attaque contre un composant et/ou un algorithme utilisant de telles clés secrètes.

Au cours de l'étape E1 d'analyse, on évalue la force des clés de l'ensemble des clés possibles vis-à-vis de l'attaque identifiée. Puis on classe les clés de l'ensemble de clés selon un ordre de force décroissant.

Dans le cas où plusieurs attaques sont identifiées, on détermine au cours de l'étape E1 la force des clés vis-à-vis de chaque attaque identifiée. Ensuite, on détermine la force résultante d'une clé comme étant le minimum des forces de cette clé vis-à-vis de l'ensemble des attaques identifiées. Enfin, on classe les clés de l'ensemble de clés selon un ordre de force résultante décroissant.

Au cours de l'étape E2 d'extraction d'un sous-ensemble de clés, dans le cas où une seule attaque est identifiée, on extrait un nombre de clés suffisant parmi les clés les plus fortes de l'ensemble de clés possibles. Selon une première variante, le nombre de clés extraites est fixé. Selon une

autre variante, le nombre de clés à extraire est fonction de la force moyenne des clés extraites, comme on le verra mieux par la suite dans un exemple.

Au cours de l'étape E2 d'extraction d'un sous-ensemble de clés, dans le cas où plusieurs attaques sont identifiées, on extrait un nombre de clés suffisant parmi les clés dont les forces résultantes sont les plus grandes parmi l'ensemble de clés possibles. Selon une première variante, le nombre de clés extraites est fixé. Selon une autre variante, le nombre de clés à extraire est fonction de la valeur moyenne de la force résultante des clés extraites.

Au cours de l'étape E3 de génération de la clé secrète, la clé secrète est choisie aléatoirement parmi le sous-ensemble de clés. La clé ainsi obtenue est mémorisée finalement dans une mémoire non volatile du composant à personnaliser.

La clé secrète obtenue selon le procédé de l'invention est ainsi nécessairement une clé forte vis-à-vis de l'attaque ou des attaques identifiées. L'attaque identifiée ne donne donc pas de résultat si elle est appliquée à un composant utilisant ladite clé secrète. Par ailleurs, ladite clé secrète ayant été choisie dans le sous-ensemble de clés comprenant un nombre suffisant de clés, une recherche exhaustive ne donne pas non plus de résultat.

Le procédé de l'invention permet ainsi de générer des clés telles que l'attaque identifiée ou la recherche exhaustive appliquée sur un composant utilisant la clé ne peut aboutir.

L'invention peut être appliquée pour la génération de clés secrètes pour tout algorithme pour lequel au moins une attaque possible est identifiée, et pour lequel les clés sont plus ou moins sensibles vis-à-vis de l'attaque identifiée. Dans un exemple de réalisation, l'invention est appliquée à l'algorithme Comp128.

L'invention et les avantages qui en découlent apparaîtront plus clairement à la lecture de la description qui suit. Un exemple de mise en oeuvre d'un procédé de génération de clés sécurisées sera donné. La description est à lire en référence aux dessins annexés dans lesquels :

- la figure 1 est un schéma bloc d'une architecture d'un dispositif dans lequel est implanté le procédé de l'invention, et
- la figure 2 est un diagramme d'un procédé selon l'invention.

La figure 1 représente sous forme de schéma bloc un dispositif électronique 1 apte à mettre en oeuvre un procédé de génération de clés selon l'invention. Dans l'exemple, le dispositif 1 est un lecteur destiné à la personnalisation de cartes à puce de type cartes SIM. Le dispositif 1 comprend une interface de communication 10 et des moyens de calcul programmés composés d'une unité centrale 2 reliée fonctionnellement à un ensemble de mémoires dont :

- une mémoire 4 accessible en lecture seulement, dans l'exemple du type ROM masque, aussi connue sous l'appellation anglaise "mask Read-Only Memory (mask ROM)",
- une mémoire 6 re-programmable électriquement, dans l'exemple du type EEPROM (de l'anglais "electrically erasable programmable ROM"), et
- une mémoire de travail 8 accessible en lecture et en écriture, dans l'exemple du type RAM (de l'anglais "Random Access Memory"). Cette mémoire comprend notamment les registres utilisés par le dispositif 1.

Le code exécutable correspondant au procédé de l'invention pour la génération de clé secrète destinée à la carte à personnaliser est contenu en mémoire programme. Ce code peut en pratique être contenu en mémoire 4, accessible en lecture seulement et/ou en mémoire 6 réinscriptible.

L'unité centrale 2 est reliée à l'interface de communication 10 qui assure l'échange des signaux avec la carte à personnaliser et l'alimentation de sa puce. L'interface de communication 10 est en contact avec la puce de la carte à personnaliser (non représentée sur la figure 1) par l'intermédiaire d'une liaison physique (carte à contact) ou d'une liaison radio-fréquence (carte sans contact).

On suppose dans l'exemple suivant que l'algorithme utilisé est le Comp128. Il utilise des clés de taille N0=128 bits composées de 8 sous-clés de 16 bits. Le nombre total de clés possibles pour cet algorithme est donc égal à $N=(2^{16})^{8}=2^{128}$ clés possibles.

Il est connu que cet algorithme est sensible à une cryptanalyse nommée "attaque par collision". Cette attaque consiste à trouver des messages clairs distincts fournissant un même message chiffré. Ce phénomène s'appelle une collision et permet de retrouver la valeur d'une sous-clé. Cette recherche de collision peut être répétée jusqu'à obtention de toutes les 16 sous-clés, c'est à dire l'obtention de la valeur de la clé secrète utilisée.

Dans la description qui suit, le procédé de l'invention produit des clés secrètes sécurisées contre cette attaque identifiée (attaque par collision).

Lors de la mise en oeuvre d'un procédé de génération de clés selon l'invention, on réalise (figure 2) les étapes suivantes :

- E1 : Analyse de l'ensemble des clés possibles ;
- E2 : Extraction d'un sous-ensemble de clés à partir dudit ensemble de clés possibles ;
- E3 : Génération d'une clé secrète à partir du sous-ensemble de clés.

La clé secrète générée peut alors être mémorisée dans une mémoire non volatile de la carte à personnaliser. Les

étapes E1 et E2 peuvent être réalisées une fois pour toutes. L'étape E3 est à répéter pour chaque carte à personnaliser.

Au cours de l'étape E1, on examine l'ensemble (IK) des clés possibles. En particulier, on évalue la force de ces clés, c'est à dire l'effort T(Ki) nécessaire à l'aboutissement de l'attaque considérée dans le cas d'une clé Ki. Cet effort est déterminé en fonction des connaissances et des performances techniques du matériel disponible que l'attaquant est supposé avoir. On classe ensuite toutes les clés par ordre décroissant de force T(Ki), de sorte que l'on ait :

$$T(Ki) \geq T(Kj) \text{ pour tout } i < j.$$

La première étape E1 permet ainsi de classer les clés selon leur force et ainsi de distinguer les clés fortes des clés faibles. L'évaluation de la force des clés ne nécessite pas d'être effectuée avec précision. De même, si la distinction entre clés fortes et clés faibles est primordiale, le classement des clés peut ne pas être fait de façon absolument rigoureuse.

Dans la deuxième étape E2, on extrait de l'ensemble IK des clés possibles un sous-ensemble SK de clés de sorte que :

- les clés du sous-ensemble SK soient aussi fortes que possible pour résister à l'attaque identifiée, et
- les clés du sous-ensemble SK soient en nombre suffisant pour résister à une recherche exhaustive.

Dans la suite, il est présenté une méthode pour optimiser le processus d'extraction du sous-ensemble de clés SK décrit dans l'étape E2. Néanmoins, une telle optimisation n'est pas obligatoire pour tirer bénéfice de l'invention. On peut en effet extraire un sous-ensemble de clés SK arbitraire et non optimal contenant suffisament de clés fortes pour contrer aussi bien l'attaque identifiée (grâce à la force des clés) que la recherche exhaustive (grâce au nombre de clés).

Concrètement, l'effort moyen à fournir pour que l'attaque identifiée aboutisse est égal à la somme des efforts à fournir pour toutes les clés du sous-ensemble SK divisée par le nombre de clés du sous-ensemble SK, soit :

$$T1=(1/NS)*\Sigma T(Ki), \text{ pour i variant entre 1 et NS,}$$

NS étant le nombre d'éléments dans le sous-ensemble de clés SK.

Par ailleurs, l'effort à fournir pour mener à son terme une recherche exhaustive sur la base du sous-ensemble SK de clés est égal à :

$$T2=NS*T0,$$

où T0 est le temps d'exécution de l'algorithme.

Dans la mesure où un attaquant peut choisir de mener une recherche exhaustive ou l'attaque identifiée, l'effort moyen à fournir pour obtenir une clé du sous-ensemble SK est donné par la formule :

$$T3=Min[T1;T2]=Min[(1/NS)*\Sigma T(Ki);NS*T0]$$

Pour durcir l'algorithme, on cherche à maximiser l'effort moyen T3. Pour cela, on insère des clés dans le sous-ensemble SK par ordre décroissant de force T(Ki), jusqu'à ce que le nombre de clés dans SK atteigne un nombre NS0 optimal.

La fonction $T1=(1/NS)*\Sigma T(Ki)$ est une fonction décroissante de NS, dans la mesure où les clés insérées dans le sous-ensemble SK ont une force décroissante. Inversement, la fonction T2=NS*T0 est une fonction croissante, linéaire de NS.

Une étude mathématique rapide permet de montrer que dans ce cas, T3 est maximum lorsque T1=T2. Ceci permet dans le cas général de calculer le nombre NS0 optimum de clés à insérer dans le sous-ensemble de clés SK selon la relation :

$$T0*(NS0)^2=\Sigma T(Ki), \text{ pour i variant entre 1 et NS0.}$$

Au cours de l'étape E3, on génère ensuite une clé secrète choisie de manière aléatoire dans le sous-ensemble de clés obtenu au cours de l'étape E2. La clé secrète choisie est

finalement mémorisée dans une mémoire non volatile du composant à personnaliser.

Dans le cas pratique d'un composant utilisant l'algorithme Comp128, une clé est composée de 8 sous-clés de 16 bits et une clé est forte si et seulement si les 8 sous-clés sont elles-même fortes.

Au cours de l'étape E1, on analyse les 2^{16} sous-clés de 16 bits et on identifie 769 d'entre elles comme étant des sous-clés fortes. Ces 769 sous-clés sont celles présentant la propriété de ne pas donner lieu aux collisions considérées par l'attaque identifiée.

L'étape E2 consiste alors à définir le sous-ensemble SK comme l'ensemble des clés dont toutes les sous-clés font partie de l'ensemble des 769 sous-clés fortes identifiées à l'étape E1.

Au cours de l'étape E3, on choisit aléatoirement 8 sous-clés dans le sous-ensemble des 769 sous-clés fortes, pour former finalement une clé secrète forte.

Les 8 sous-clés étant fortes, la clé secrète ainsi obtenue est résistante à l'attaque identifiée (attaque par collision). Par ailleurs, la clé secrète obtenue est également résistante à une recherche exhaustive car la taille du sous-espace SK (dont elle est issue) est égale à $769^8\#2^{77}$.

REVENDICATIONS

1. Procédé de génération de clés secrètes sécurisées pour un algorithme cryptographique, faisant face à une attaque qui le rend considéré comme cassé, comprenant les étapes suivantes :

E1 : analyse de l'ensemble (IK) des clés possibles ,

E2 : extraction d'un sous-ensemble (SK) de clés à partir de l'ensemble (IK),

E3 : génération des clés secrètes à partir du sous-ensemble (SK) de clés,

procédé caractérisé en ce que, au cours de l'étape (E1) d'analyse, on évalue la force des clés de l'ensemble (IK) des clés possibles vis-à-vis d'une attaque identifiée, qui rend l'algorithme inutisable.

2. Procédé selon la revendication 1, caractérisé en ce que, au cours de l'étape (E2) d'extraction d'un sous-ensemble (SK), on extrait de l'ensemble des clés (IK) un nombre suffisant de clés fortes vis-à-vis de l'attaque identifiée.

3. Procédé selon la revendication 2 caractérisé en ce que le nombre suffisant (NSO) est fixé.

4. Procédé selon la revendication 3 caractérisé en ce que le nombre suffisant est déterminé en fonction de la force moyenne des clés du sous-ensemble de clés (SK).

5. Procédé selon la revendication 1 caractérisé en ce que, face à plusieurs attaques identifiées au cours de l'étape (E1) d'analyse, on évalue la force des clés de l'ensemble des clés (IK) vis-à-vis de chacune de ces dites attaques.

6. Procédé selon la revendication 5 caractérisé en ce qu'on définit la force résultante d'une clé comme étant le minimum des forces de ladite clé vis-à-vis de toutes lesdites attaques identifiées.

7. Procédé selon l'une quelconque des revendications 1, 5 ou 6 caractérisé en ce que, au cours de l'étape (E2) d'extraction d'un sous-ensemble (SK), on extrait de l'ensemble des clés (IK) un nombre suffisant de clés fortes vis-à-vis desdites attaques identifiées.

8. Procédé selon la revendication 7 caractérisé en ce que le nombre suffisant (NSO) est fixé.

9. Procédé selon la revendication 7 caractérisé en ce que le nombre suffisant (NSO) est déterminé en fonction de la valeur moyenne des forces résultantes desdites clés vis-à-vis desdites attaques identifiées.

10. Procédé selon l'une des revendications 1 à 4 caractérisé en ce que, au cours de l'étape (E1) d'analyse, on classe ensuite les clés de l'ensemble de clés (IK) selon un ordre de force décroissant.

11. Procédé selon l'une quelconque des revendications 1, 5 à 9 caractérisé en ce que, au cours de l'étape (E1) d'analyse, on classe ensuite les clés de l'ensemble de clés (IK) selon un ordre de force résultante décroissant.

12. Dispositif pour la personnalisation d'un composant électronique par une clé secrète, choisie aléatoirement dans un sous-ensemble (SK) de clés, caractérisé en ce qu'il comprend des moyens programmés (1) pour la mise en œuvre d'un procédé selon l'une quelconque des revendications 1 à 11, les

moyens programmés comprenant notamment une unité centrale (2) et une mémoire de programme.

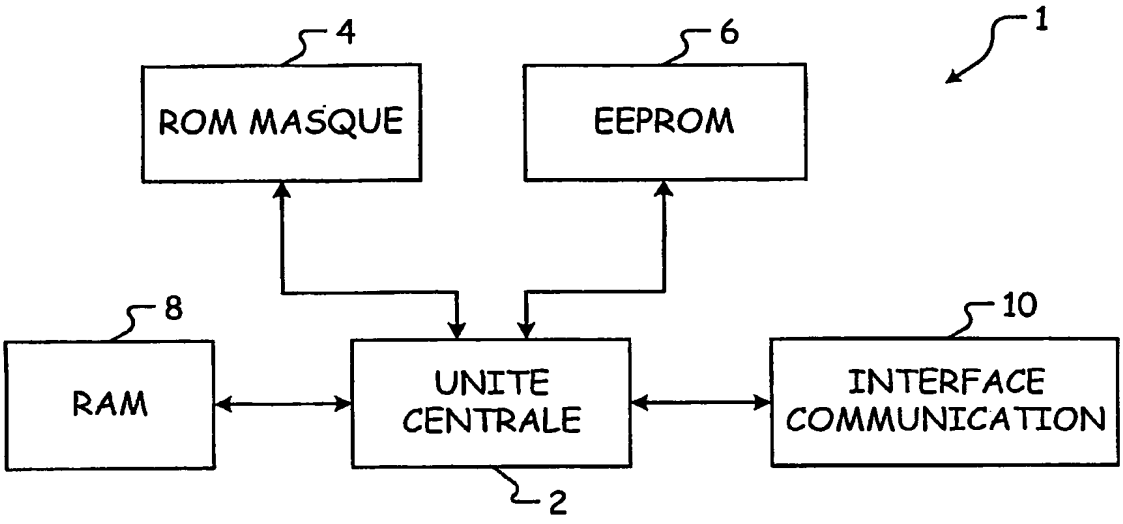

4
6
1
ROM MASQUE
EEPROM
8
10
RAM
UNITE CENTRALE
INTERFACE COMMUNICATION
2

Fig. 1

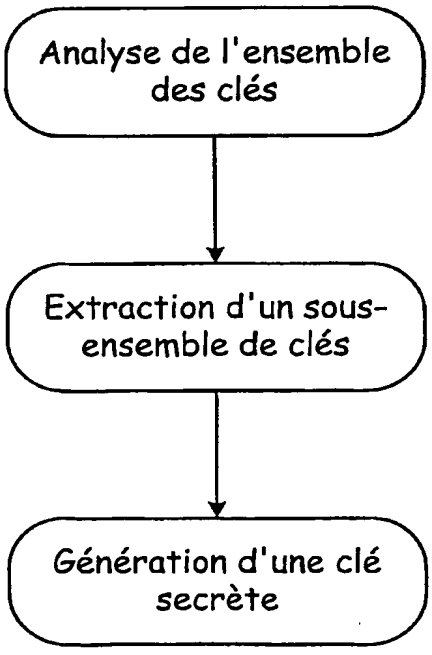

Analyse de l'ensemble des clés
Extraction d'un sous-ensemble de clés
Génération d'une clé secrète

Fig. 2

INTERNATIONAL SEARCH REPORT

Inte ial Application No
PCT/FR 03/00369

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 H04L9/06

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)
WPI Data, PAJ, EPO-Internal, INSPEC

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	A. MENEZES ET AL.: "HANDBOOK OF APPLIED CRYPTOGRAPHY" 1997 , CRC PRESS , BOCA RATON XP002219382	1
A	page 256, paragraph 7.4.3 -page 259, line 12	12
X	HEYS H M: "Linearly weak keys of RC5" ELECTRONICS LETTERS, IEE STEVENAGE, GB, vol. 33, no. 10, 8 May 1997 (1997-05-08), pages 836-837, XP006007465 ISSN: 0013-5194 abstract page 836, right-hand column, line 26 -page 837, left-hand column, paragraph 1	1,10

-/--

[X] Further documents are listed in the continuation of box C. [ ] Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier document but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
4 July 2003	14/07/2003

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Holper, G

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

Inte ıal Application No
PCT/FR 03/00369

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication,where appropriate, of the relevant passages	Relevant to claim No.
X	KOBLITZ: "ADVANCES IN CRYPTOLOGY-CRYPTO'96, IMPROVED DIFFERENTIAL ATTACKS ON RC5" 1996 , SPRINGER , BERLIN XP002219383 page 225, last paragraph -page 228, last line	1

RAPPORT DE RECHERCHE INTERNATIONALE

Der ternationale No
PCT/FR 03/00369

A. CLASSEMENT DE L'OBJET DE LA DEMANDE
CIB 7 H04L9/06

Selon la classification internationale des brevets (CIB) ou à la fois selon la classification nationale et la CIB

B. DOMAINES SUR LESQUELS LA RECHERCHE A PORTE

Documentation minimale consultée (système de classification suivi des symboles de classement)
CIB 7 H04L

Documentation consultée autre que la documentation minimale dans la mesure où ces documents relèvent des domaines sur lesquels a porté la recherche

Base de données électronique consultée au cours de la recherche internationale (nom de la base de données, et si réalisable, termes de recherche utilisés)
WPI Data, PAJ, EPO-Internal, INSPEC

C. DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie °	Identification des documents cités, avec, le cas échéant, l'indication des passages pertinents	no. des revendications visées
X	A. MENEZES ET AL.: "HANDBOOK OF APPLIED CRYPTOGRAPHY" 1997 , CRC PRESS , BOCA RATON XP002219382	1
A	page 256, alinéa 7.4.3 -page 259, ligne 12	12
X	HEYS H M: "Linearly weak keys of RC5" ELECTRONICS LETTERS, IEE STEVENAGE, GB, vol. 33, no. 10, 8 mai 1997 (1997-05-08), pages 836-837, XP006007465 ISSN: 0013-5194 abrégé page 836, colonne de droite, ligne 26 -page 837, colonne de gauche, alinéa 1	1,10

-/--

[X] Voir la suite du cadre C pour la fin de la liste des documents

[ ] Les documents de familles de brevets sont indiqués en annexe

° Catégories spéciales de documents cités:

"A" document définissant l'état général de la technique, non considéré comme particulièrement pertinent

"E" document antérieur, mais publié à la date de dépôt international ou après cette date

"L" document pouvant jeter un doute sur une revendication de priorité ou cité pour déterminer la date de publication d'une autre citation ou pour une raison spéciale (telle qu'indiquée)

"O" document se référant à une divulgation orale, à un usage, à une exposition ou tous autres moyens

"P" document publié avant la date de dépôt international, mais postérieurement à la date de priorité revendiquée

"T" document ultérieur publié après la date de dépôt international ou la date de priorité et n'appartenenant pas à l'état de la technique pertinent, mais cité pour comprendre le principe ou la théorie constituant la base de l'invention

"X" document particulièrement pertinent; l'invention revendiquée ne peut être considérée comme nouvelle ou comme impliquant une activité inventive par rapport au document considéré isolément

"Y" document particulièrement pertinent; l'invention revendiquée ne peut être considérée comme impliquant une activité inventive lorsque le document est associé à un ou plusieurs autres documents de même nature, cette combinaison étant évidente pour une personne du métier

"&" document qui fait partie de la même famille de brevets

Date à laquelle la recherche internationale a été effectivement achevée	Date d'expédition du présent rapport de recherche internationale
4 juillet 2003	14/07/2003

Nom et adresse postale de l'administration chargée de la recherche internationale	Fonctionnaire autorisé
Office Européen des Brevets, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Holper, G

RAPPORT DE RECHERCHE INTERNATIONALE

Der Internationale No
PCT/FR 03/00369

C.(suite) DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie *	Identification des documents cités, avec,le cas échéant, l'indicationdes passages pertinents	no. des revendications visées
X	KOBLITZ: "ADVANCES IN CRYPTOLOGY-CRYPTO'96, IMPROVED DIFFERENTIAL ATTACKS ON RC5" 1996 , SPRINGER , BERLIN XP002219383 page 225, dernier alinéa -page 228, dernière ligne	1